Virtualisierung und Cloud Computing unter dem Aspekt Sicherheit

Dr. Daniel Hamburg

Herausforderungen

- Komplexes und vielschichtiges Thema
  - Über 250 M Google Hits, fast 1 M Google Scholar Hits
- Unternehmenssicht
  - Keine Plar n Wiese sondern Migration klassischer IT-Infrastrukturen
    1. Iden ualisierung und Cloud Computing veränderten grun heitsmaßnahmen
    2. Able der Sicherheitsmaßnahmen

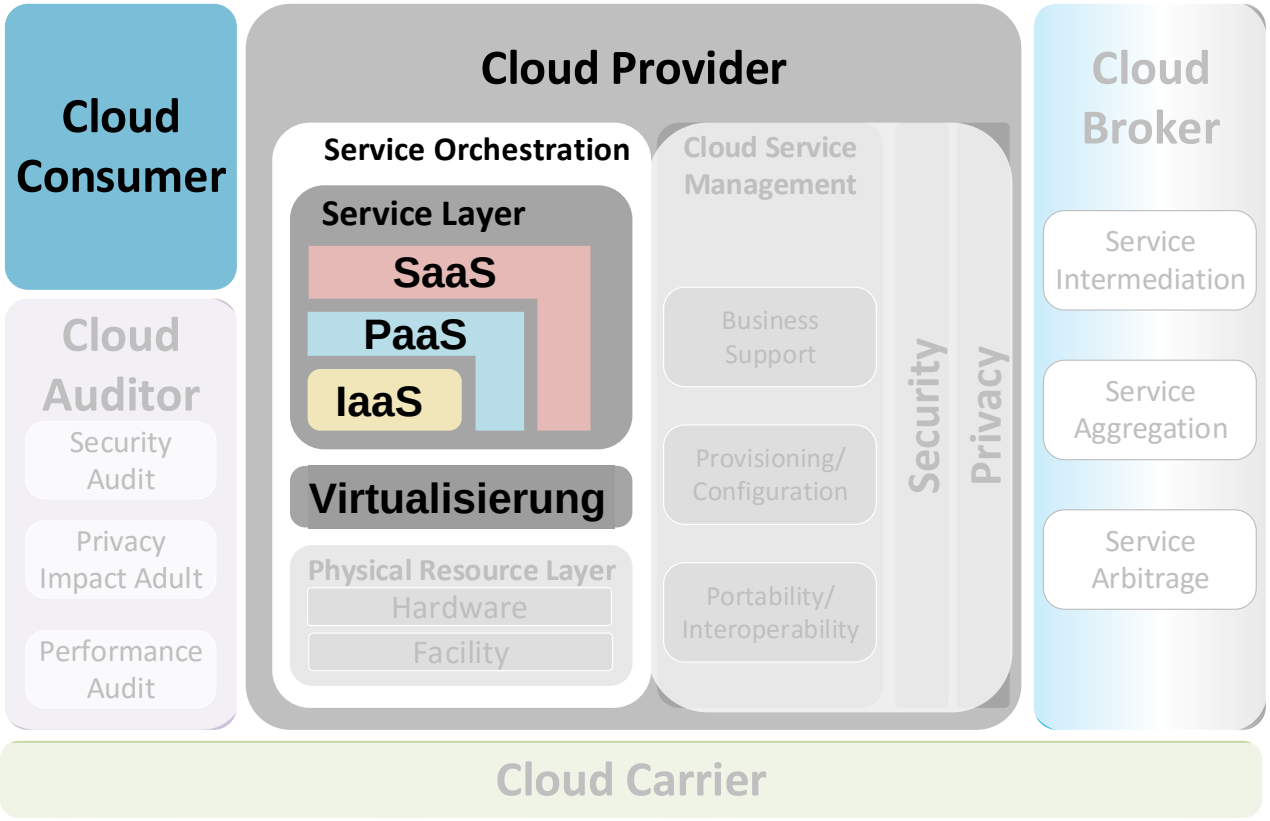
➔ Divide and conquer

Agenda

1	Rekapitulation Cloud Computing und Virtualisierung
2	Fallbeispiel VitualCloudReady GmbH (VCR)
3	Zusammenfassung

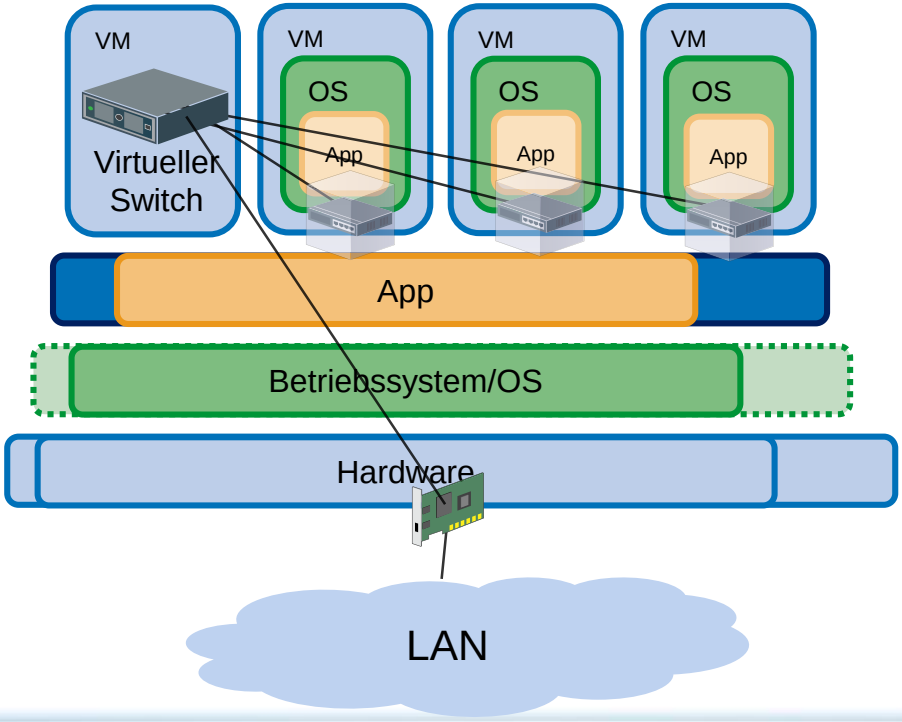
Cloud Computing

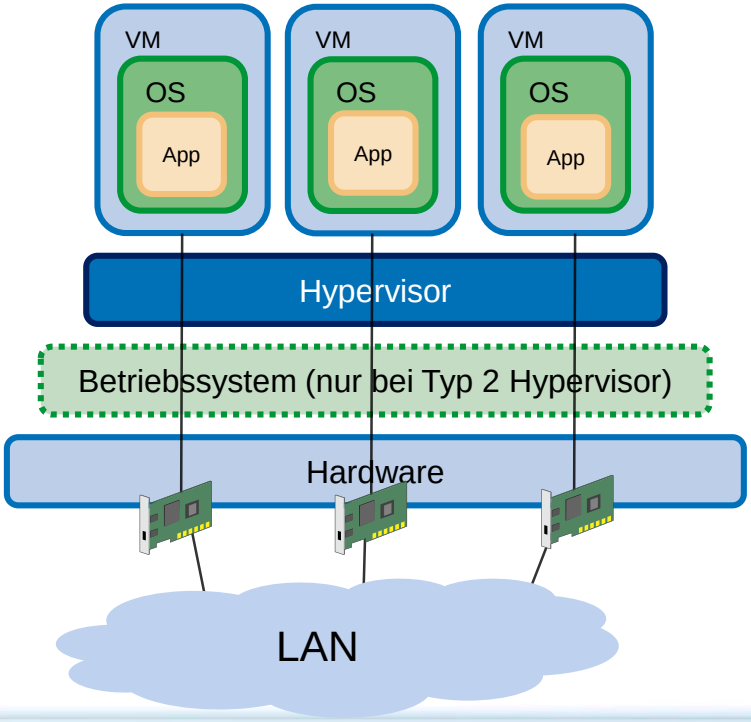
- Bedarfsorientierter netzbasierter Zugriff auf geteilten Pool von konfigurierbaren Rechnerressourcen (NIST)
- Liefermodelle: private, community, public



Virtualisierung

- Häufigste Ausprägung
  - Systemvirtualisierung auf Hardwareebene = Simulation von Hardware mittels eines Hypervisors
  - Netzwerk: physikalisch oder virtuell

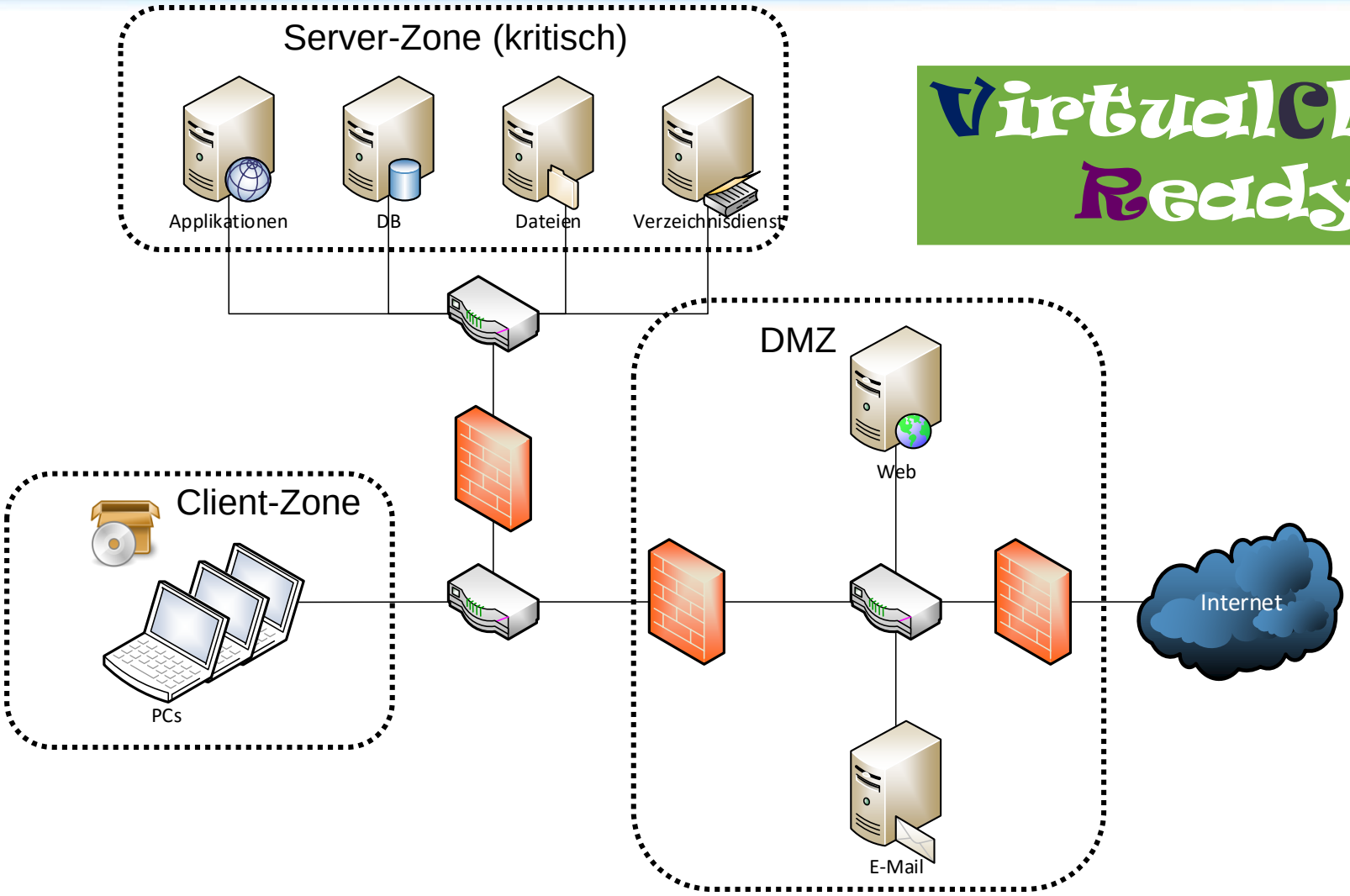




Agenda

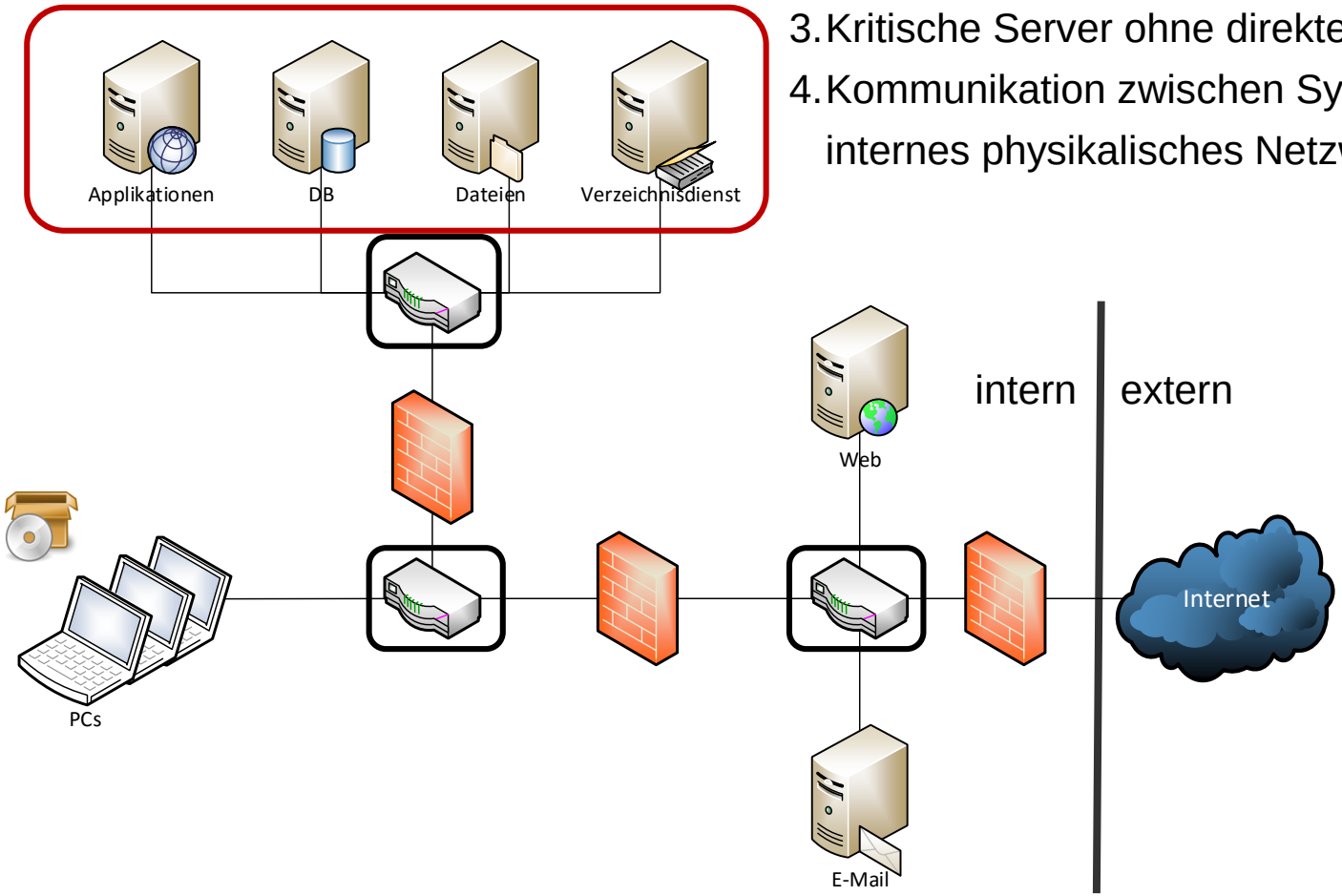
Agenda

IT-Infrastruktur der VCR

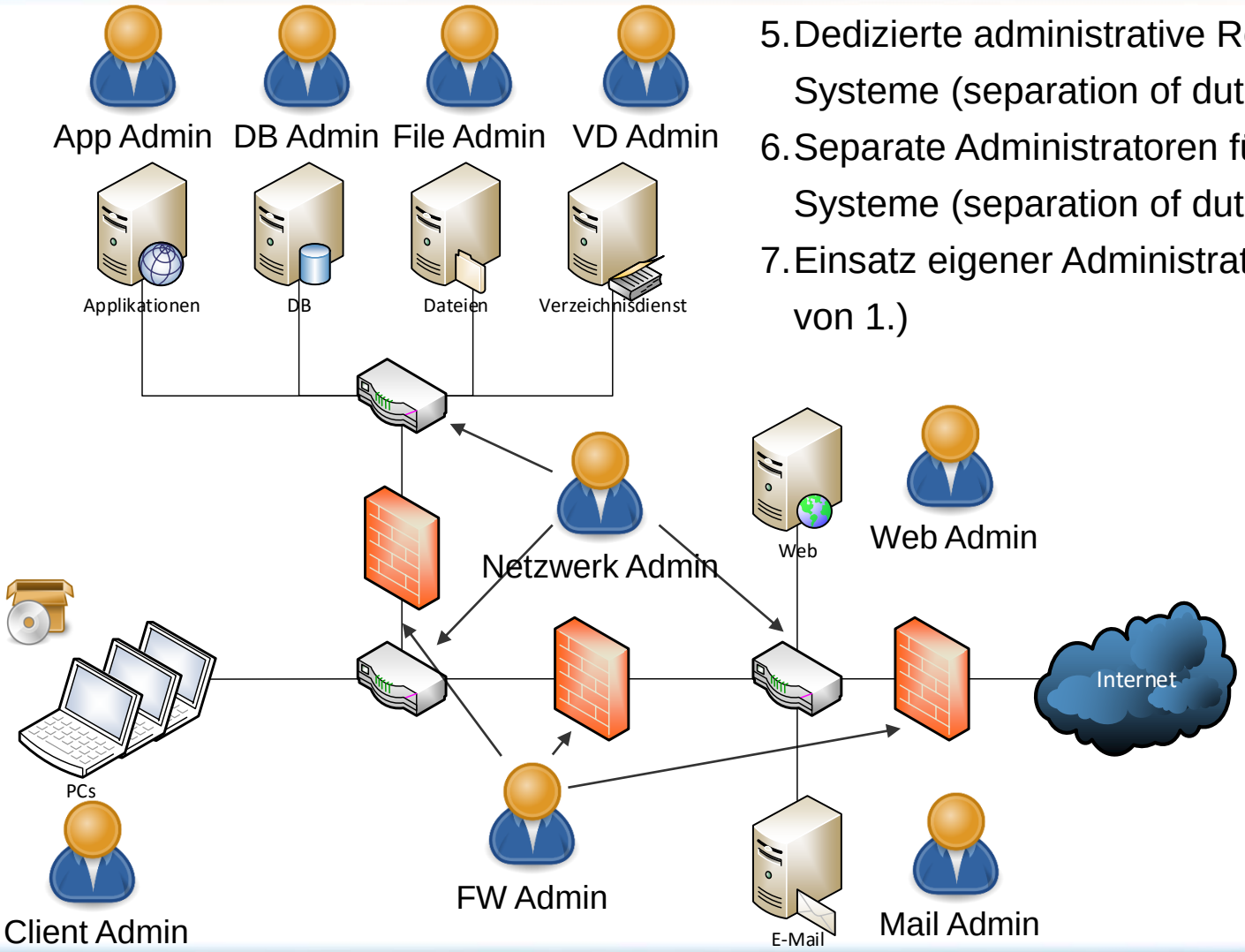


Sicherheitstechnische Eigenschaften: Kommunikation und Schutz vor Externen

1. Sicherheitsniveau unabhängig von Externen
2. Klare Außengrenzen und Trennung intern/extern
3. Kritische Server ohne direkten Internetzugang
4. Kommunikation zwischen Systemen erfolgt über internes physikalisches Netzwerk



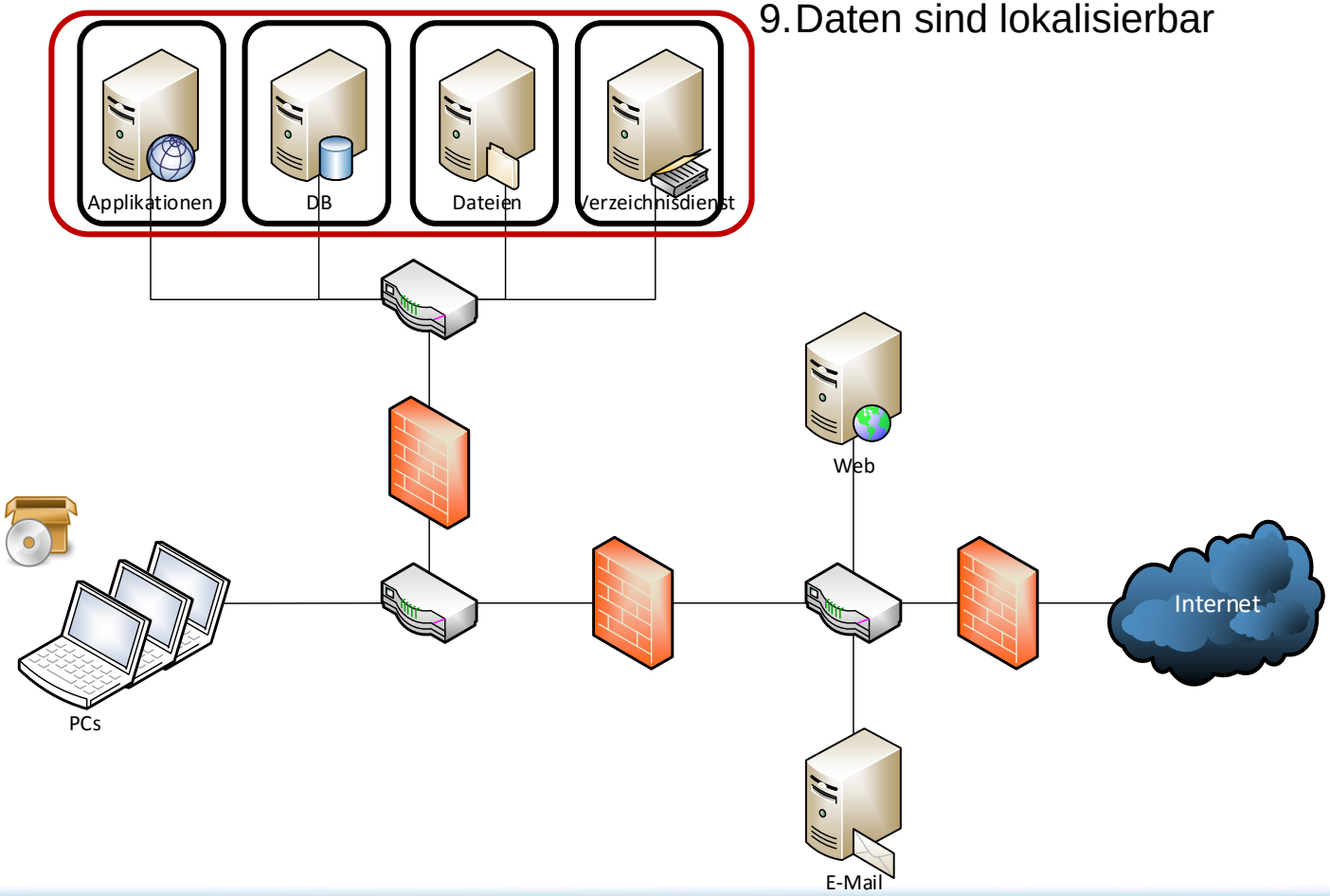
Sicherheitstechnische Eigenschaften: Administration



5. Dedizierte administrative Rechte für einzelne Systeme (separation of duties)
6. Separate Administratoren für Netzwerk und Systeme (separation of duties)
7. Einsatz eigener Administratoren (Speziallfall von 1.)

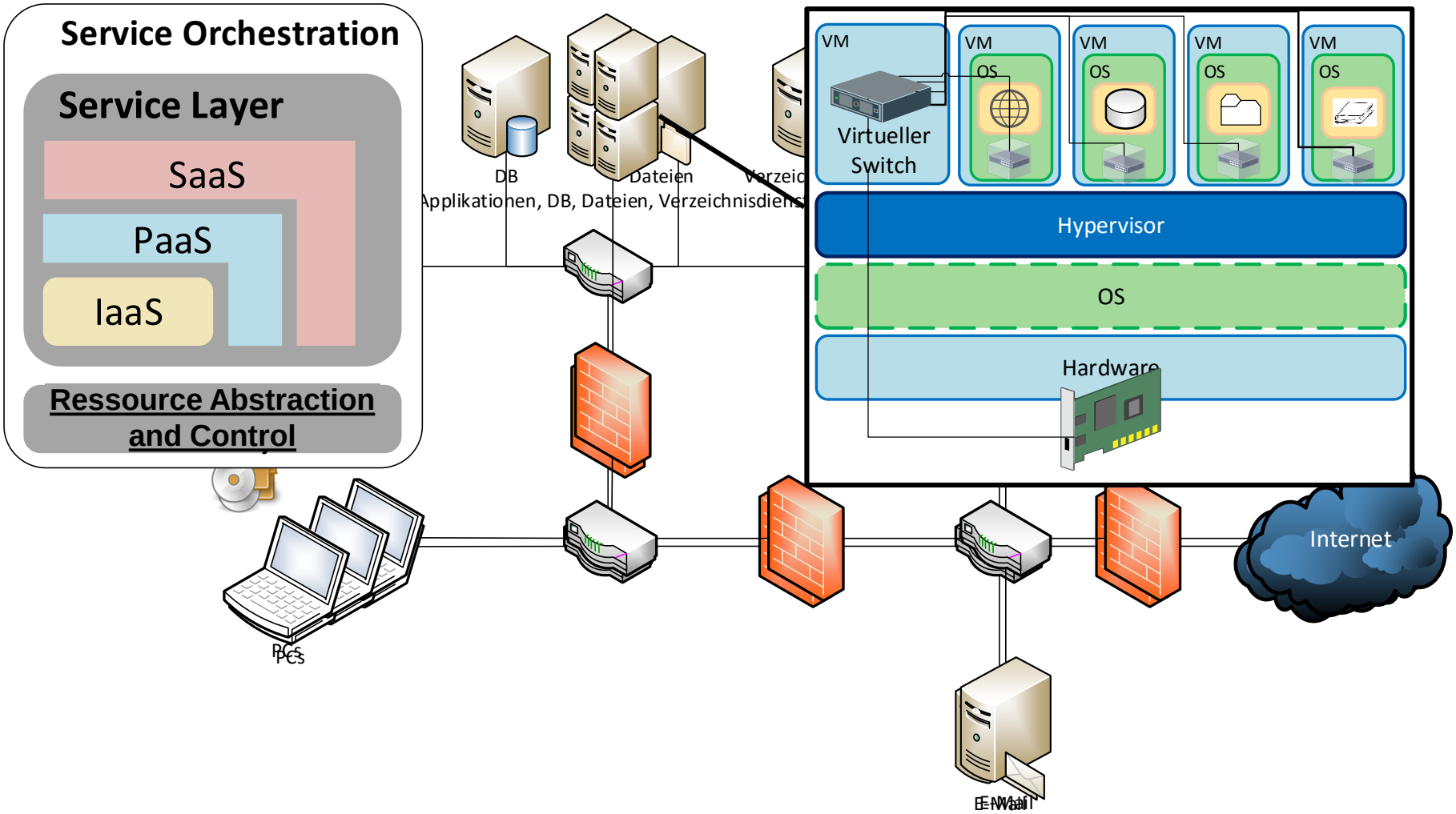
Sicherheitstechnische Eigenschaften: Daten

8. Verteilung kritischer Daten auf mehrere Systeme ➔ Kein Single point of failure/ attack
9. Daten sind lokalisierbar



Agenda

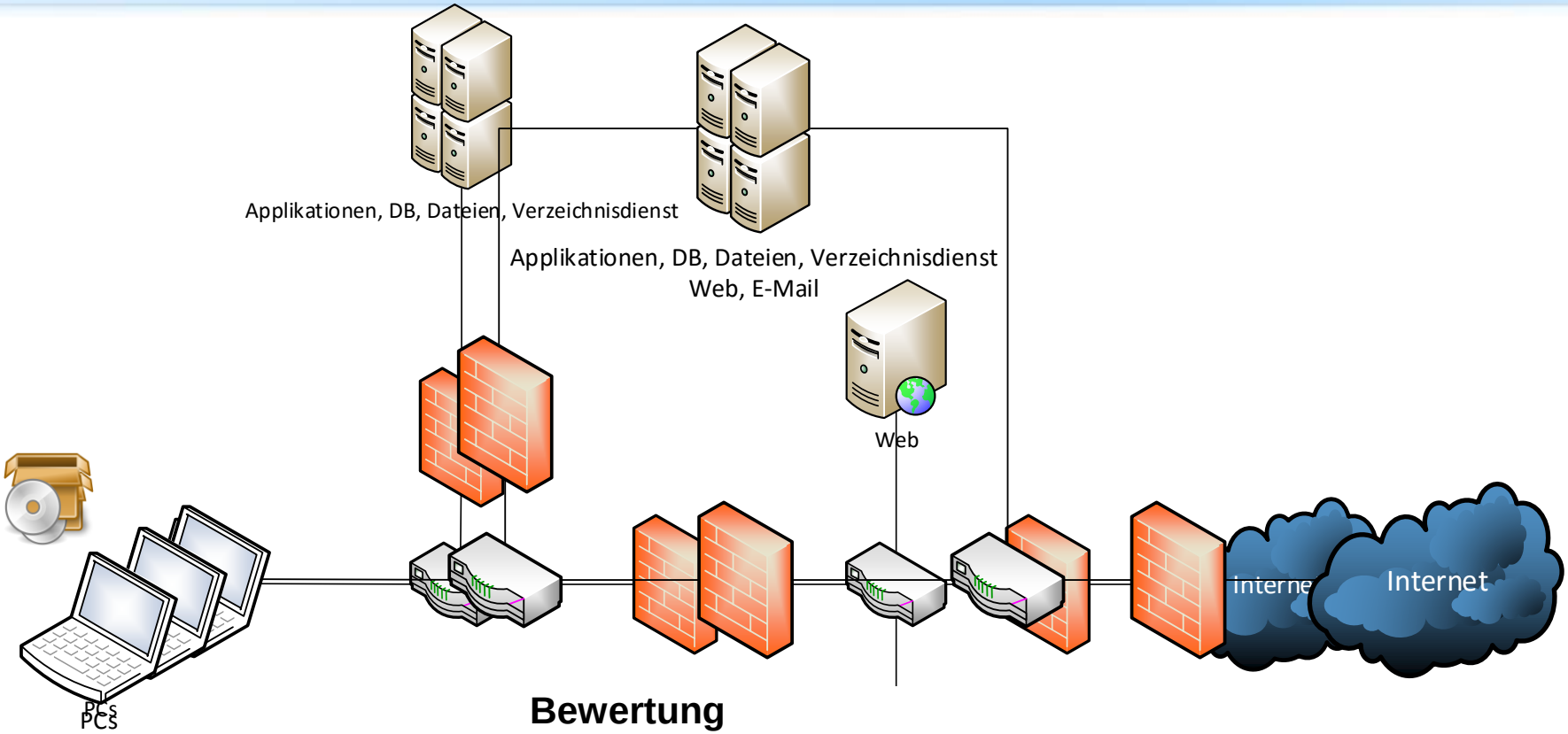
Virtualisierung der internen Server



Virtualisierung der internen Server: Veränderte Sicherheitseigenschaften

Sicherheitseigenschaften initial	Veränderte Sicherheitseigenschaften
4. Kommunikation zwischen Systemen erfolgt über internes physikalisches Netzwerk	Inter-Server Kommunikation über virtuelles Netzwerk (erschwerte Überwachung und Kontrolle)
5. Dedizierte administrative Rechte für einzelne Systeme (separation of duties)	Administrativer Zugriff auf Hypervisor = Voller Zugriff auf alle kritischen Server
6. Separate Administratoren für Netzwerk und Systeme (separation of duties)	Administrativer Zugriff auf Hypervisor = Vereinigung System- und Netzwerk-administration (virtuelles Netzwerk) für kritische Server
8. Verteilung kritischer Daten auf mehrere Systeme ➔ Kein Single point of failure/ attack	• Zentrale Server-Hardware bestimmt Verfügbarkeit aller 4 kritischen Server (single point of failure) • Sicherheit des Hypervisors und OS bestimmt Sicherheitsniveau aller 4 Server (single point of attack)

Virtualisierung der gesamten Server-Landschaft



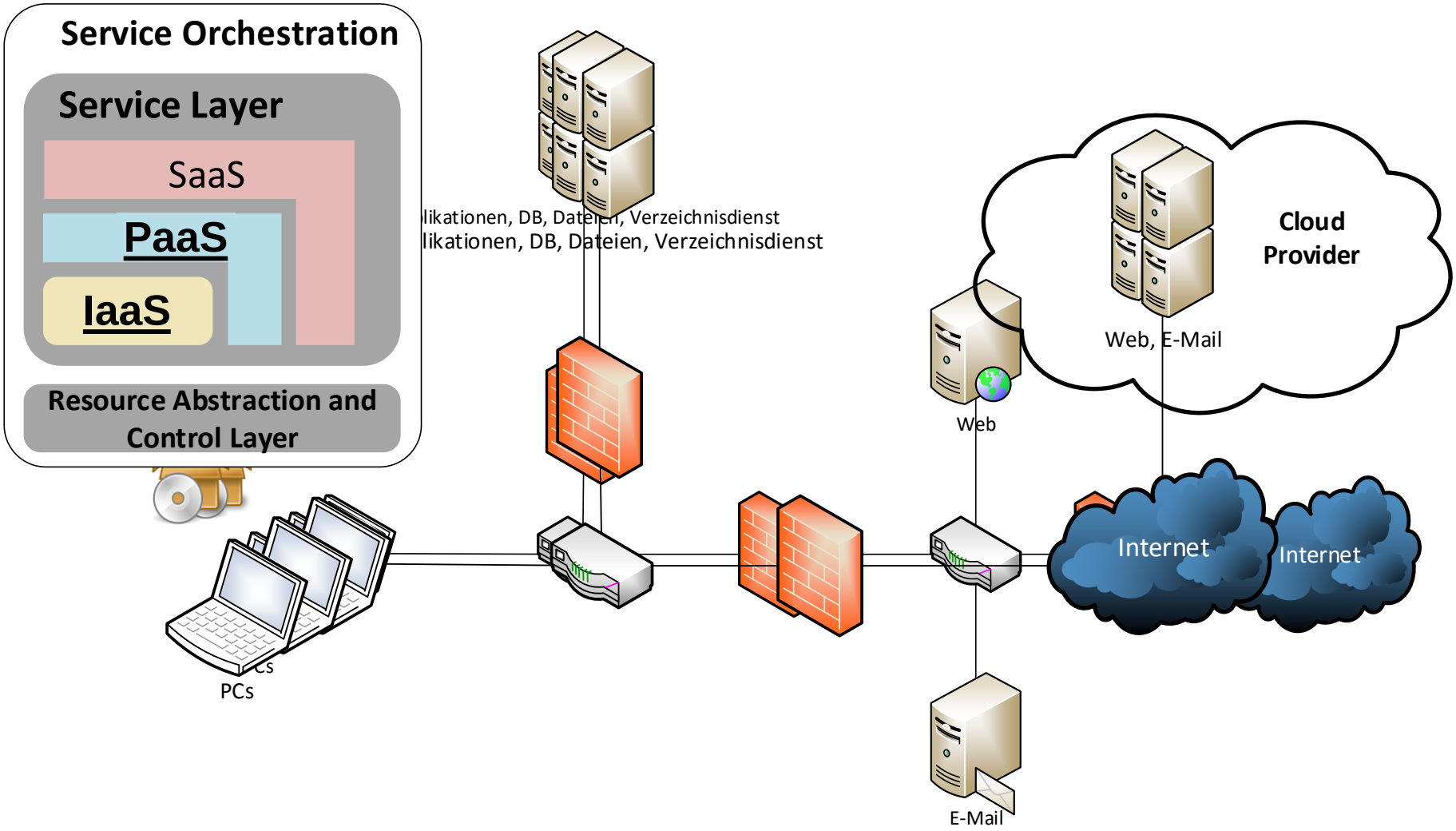
Bewertung

- Sonderfall der Server-Virtualisierung jedoch Zusammenlegung DMZ und Server-Zone!

➔ Virtualisierungslösung muss gleiches Sicherheitsniveau bieten wie physikalische Trennung

Agenda

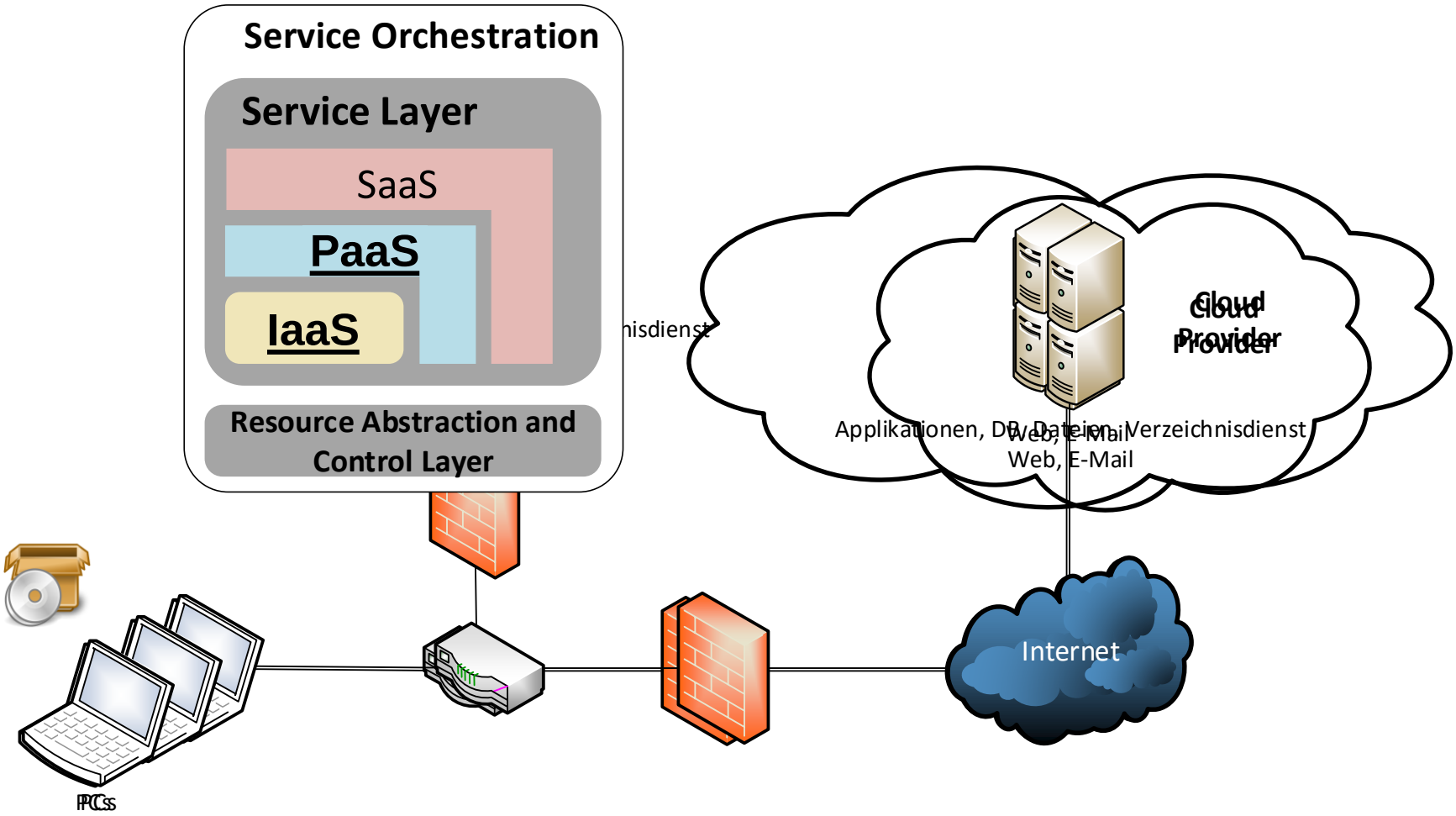
DMZ bei Cloud Provider



DMZ beim Cloud Provider: Veränderte Sicherheitseigenschaften

Sicherheitseigenschaften initial	Veränderte Sicherheitseigenschaften
1. Sicherheitsniveau unabhängig von Externen	Abhängigkeit vom Provider und seinem Sicherheitsniveau, z. B. Schutz vor Externen, Mandantentrennung, Abhängigkeit von Partnern
2. Klare Außengrenzen und Trennung intern/extern	Aufhebung der Grenzen (erschwerte Überwachung und Kontrolle)
4. Kommunikation zwischen Systemen erfolgt über internes physikalisches Netzwerk	Interner Verkehr (Daten und Administration) über das Internet
7. Einsatz eigener Administratoren (Speziallfall von 1.)	Zugriff durch Mitarbeiter des Cloud Providers inkl. potentiellem Zugriff auf sensitive Daten

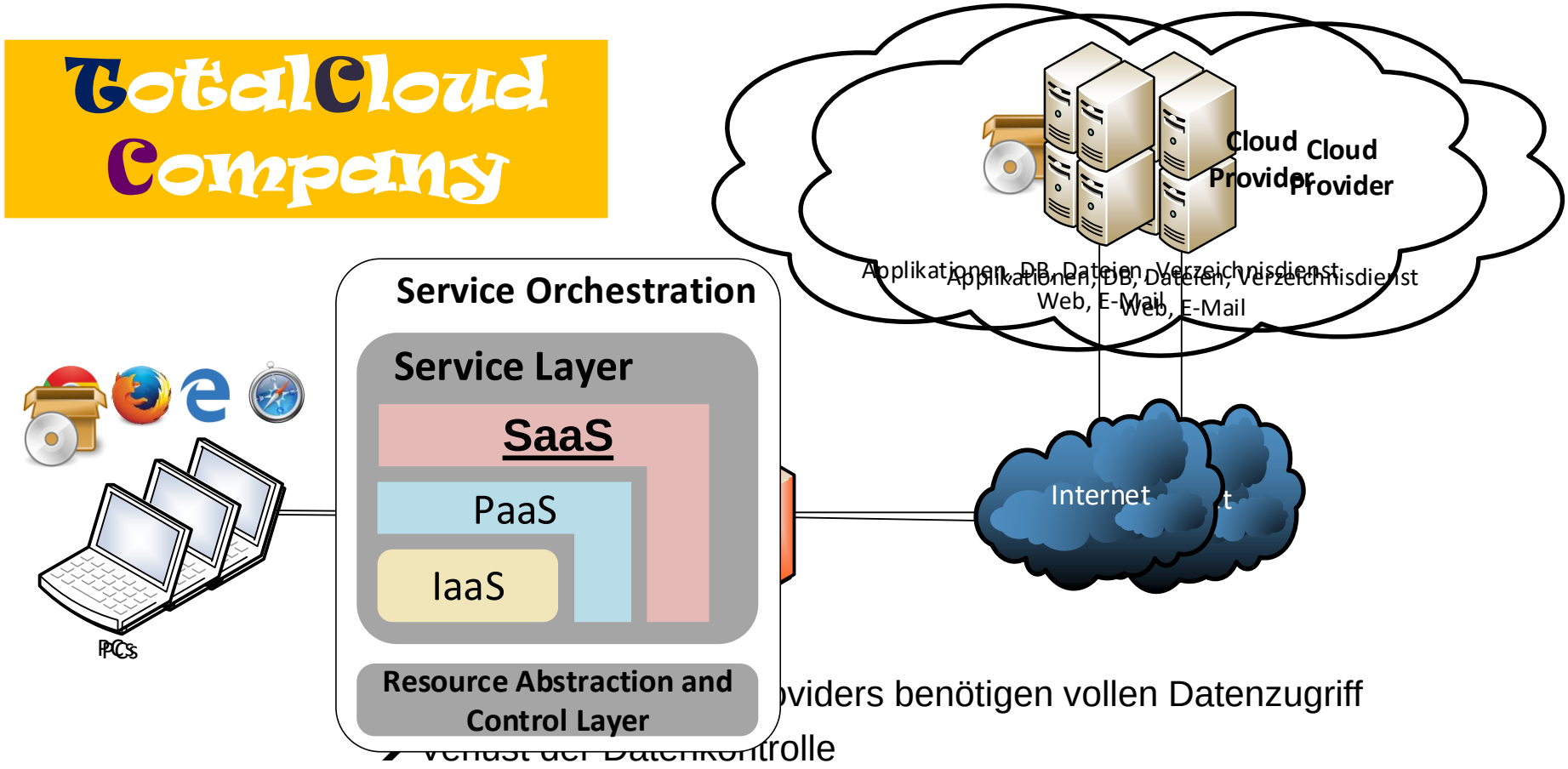
Alle Server bei Cloud Provider



Alle Server beim Cloud Provider: Veränderte Sicherheitseigenschaften

Sicherheitseigenschaften initial	Veränderte Sicherheitseigenschaften
3. Kritische Server ohne direkten Internetzugang	Server müssen aus dem Internet erreichbar sein
9. Daten sind lokalisierbar	• Daten i.d.R. nicht mehr lokalisierbar • Potentielle Datenschutzprobleme, z. B. bei Löschung, Verschiebung

Applikationen bei Cloud Provider



oviders benötigen vollen Datenzugriff

Verlust der Datenkontrolle

Agenda

1	Rekapitulation Cloud Computing und Virtualisierung
2	Fallbeispiel VitualCloudReady GmbH (VCR)
3	Zusammenfassung

Zusammenfassung

- Migration zu Virtualisierung und Cloud Computing führt zur Veränderung von Sicherheitseigenschaften
- Einsatz entsprechender organisatorischer, prozessualer und technischer Sicherheitsmaßnahmen zur Aufrechterhaltung des Sicherheitsniveaus notwendig
- Neben den veränderten Sicherheitseigenschaften kann der Einsatz eines Cloud Providers aber auch sicherheitstechnische Vorteile bringen
  - Hohe Verfügbarkeit aufgrund Elastizität
  - Hohes Sicherheitsniveau durch effiziente Sicherheitsmechanismen und -prozesse